REMARKS

Claims 1-13 have been canceled without prejudice or disclaimer. Claims 14-27 are newly presented and are the pending claims.

Priority

Applicants appreciate the Examiner's acknowledgment of the claim for priority and receipt of the priority document.

35 U.S.C. §112

Applicants have amended the description on page 63 of the specification, which was identified by the Examiner, to ensure compliance with 35 USC § 112, first paragraph.

Claim 5 has been canceled without prejudice or disclaimer thereby rendering the rejection under 35 USC § 112, second paragraph moot. New claims 14-27 have been presented that comply with 35 USC § 112.

35 U.S.C. §§102 and 103

The rejection of claims 8-13 under 35 U.S.C. § 102 as being anticipated by Deo et al and the rejection of claims 1-7 under 35 U.S.C. § 103 as being unpatentable over Morris in

view of Inoue are rendered moot by the cancellation without prejudice or disclaimer of these claims. New claims 14-27 are patentable over the references relied upon in these rejections and the remainder of the art of record for the following reasons.

Newly presented claims 14-27 include independent claim 14 and claims 15-19 which depend from claim 14 as a base claim; and independent claim 21 as well as dependent claims 22-27 which depend on claim 21 as a base claim. Claims 14-20 are supported by Figs. 26 and 27 of the application which show an interrogator, and the description on page 27, line 22 to page 29, line 16 and on page 38, line 12 to page 39, line 17 of the specification. New claims 21-27 are supported by Figs. 34-37 of the application which show a facility to execute service having a computer system (see the description from page 46, line 2 to page 51, line 2 of the specification).

In general, the present invention is directed to reduce forgery of certificates, such as bank notes, money coupons, etc. that might be fraudulently created using copiers or high-quality printers. This is accomplished by using IC chips as electronic tags that are attached to a medium constituting the

certificate. Since IC chips must be manufactured at factories equipped with semiconductor production facilities, certificates with the electronic tags are difficult to forge. Further, by including encryption technology, forgery of the certificates is made quite difficult.

Fig. 19 shows an example of a certificate, which is a Japan yen note that includes an IC chip 1908 directly placed on or buried in the certificate 1902. Fig. 20 shows an arrangement in which the IC chip is attached on a tape and other information are printed on the tape. Fig. 23 shows an example of an insurance certificate in which the certificate 2301 has the name of the insurance company 2310 printed thereon and a IC chip-attached seal 2308. The value of a digital signature 2306 are also printed on the certificate shown in Fig. 23.

In accordance with the invention, a digital signature, which is encrypted by a secret key, is created from important information to be printed on the surface of a certificate. Such information can be the name for a passport or the amount of money for a bank note, etc. Further, the information is stored in the electronic tag attached to the certificate. The

digital signature is printed on the certificate and when the certificate is to be authenticated, the digital signature printed on the certificate and the stored information in the electronic tag are processed to obtain values corresponding to the important information printed on the certificate. If the values are identical to the information printed on the certificate, the certification process determines that the certificate is authentic. *See* page 4, lines 15-28 and page 29, lines 10-31, of the specification.

Deo discloses a smart card 10 and a terminal 32. Smart card 10 sends its card-related certificate 40 to terminal 32 and the terminal sends its terminal-related certificate 42 to smart card 10 for authentication purposes. Further, in another authentication phase, a user is requested to enter a PIN 50. Further, an application certificates 46, 48, which are associated with selected applications are exchanged between the terminal and the smart card over an encrypted channel. Accordingly, several levels of authentication are disclosed in Deo. See, column 5, lines 45-55 and column 8, line 7 to column 10, line 30 of the reference, for example.

In Morris, a message and a message digest generated by hashing the message are encrypted by a secret key to generate a digital signature. Further, a PIN is encrypted by the user's public key to generate authentication information which is then stored in a removable memory. The removable memory is inserted into an electronic device and the authentication information is decrypted using the secret key. In this manner, the message encrypted by the secret key, the message digest and the PIN are obtained. If the decrypted PIN and the entered PIN correspond, the encrypted message and the message digest are decrypted using the public key. If the message digest generated by hashing the decrypted message and the decrypted message digest correspond, the user is allowed to access the electronic device, thereby completing the authentication processing. *See*, column 4, line 43 to column 5, line 34 with reference to Figs. 3 and 4 of Morris.

In Inoue, a non-contact IC card and terminal device is disclosed that is started by receipt of a startup drive from the terminal. Then, normal data transmission is performed between the terminal and the card. Factors are changed to increase the receiving sensitivity in a data communication

step for transmitting and receiving the data signal after transmitting/receiving the startup signal.

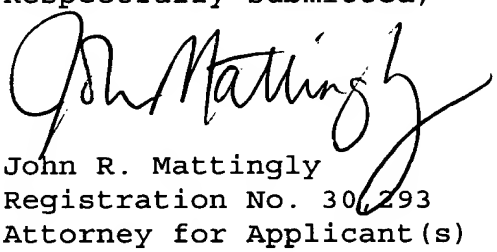
None of Deo, Morris or Inoue disclose or suggest the claimed combination of the invention set forth in the newly presented claims. In particular, independent claim 14 sets forth that third information is calculated from first information, stored in an electronic tag and received by an interrogator through an antenna, and the digital signature that is printed on the surface of a certificate, using RSA. The certificate is certified by comparing the second information that is printed on the surface of the certificate with the calculated third information. Independent claim 21 sets forth that the first information from the electronic tag and the second information printed on the surface of the certificate, along with the digital signature, are sent to a computer system which stores a public key. The claim also requires that the third information is calculated from the first information received from the electronic tag and the digital signature using RSA, followed by comparing the second information with the third information in order to certify the certificate.

None of the remainder of the art of record is sufficient to disclose or render obvious the invention as claimed. Further, each of the dependent claims sets forth additional limitations that are not disclosed or suggested by the art of record. Accordingly, Applicants respectfully assert that claims 14-27 are patentable over the art of record.

Conclusion

In view of the foregoing amendments and remarks, Applicants contend that the above-identified application is now in condition for allowance. Accordingly, reconsideration and reexamination is requested.

Respectfully submitted,



John R. Mattingly
Registration No. 30,293
Attorney for Applicant(s)

MATTINGLY, STANGER & MALUR
1800 Diagonal Rd., Suite 370
Alexandria, Virginia 22314
(703) 684-1120
Date: August 23, 2004